BOISE MATTHEWS DONEGAN LLP
Bridget M. Donegan, OSB No. 103753
805 SW Broadway, Suite 1900
Portland, OR 97205
(503) 228-0487
bridget@boisematthews.com

Attorneys for Plaintiff Loujain Hathloul Alhathloul

FOLEY HOAG LLP
Christopher E. Hart, MA BBO No. 625031
chart@foleyhoag.com
Anthony D. Mirenda, MA BBO No. 550587
adm@foleyhoag.com
Andrew Loewenstein, MA BBO No. 648074
aloewenstein@foleyhoag.com
155 Seaport Boulevard
Boston, MA 02210
(617) 832-1232

Attorneys for Plaintiff Loujain Hathloul Alhathloul

ELECTRONIC FRONTIER FOUNDATION
David Greene, CA Bar No. 160107
davidg@eff.org
Sophia Cope, CA Bar No. 233428
sophia@eff.org
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Attorneys for Plaintiff Loujain Hathloul Alhathloul

CENTER FOR JUSTICE AND ACCOUNTABILITY
Daniel McLaughlin, CA Bar No. 315326 (*pro hac vice pending)*
dmclaughlin@cja.org
Claret Vargas, MA BBO No. 679565 (*pro hac vice pending)*
cvargas@cja.org
Carmen Cheung Ka Man, NY Bar No. 4132882 *(pro hac vice pending)*
ccheung@cja.org
268 Bush St. #3432
San Francisco, CA 94104
(415) 544-0444

Attorneys for Plaintiff Loujain Hathloul Alhathloul

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

LOUJAIN HATHLOUL ALHATHLOUL,

Plaintiff,

v.

DARKMATTER GROUP,
MARC BAIER,
RYAN ADAMS, and
DANIEL GERICKE

Defendants.

Case No. 3:21-cv-01787-IM

FIRST AMENDED COMPLAINT
(Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Alien Tort Statute, 28 U.S.C. § 1350)

DEMAND FOR JURY TRIAL

PRELIMINARY STATEMENT

1. Plaintiff Loujain Hathloul Alhathloul is a preeminent Saudi human rights activist and leader of the movement to promote the rights of women and girls in the Kingdom of Saudi Arabia ("Saudi Arabia"). This action arises out of the unlawful actions by Defendant DarkMatter Group ("DarkMatter") and its former senior executives, Defendants Marc Baier, Ryan Adams, and Daniel Gericke, to hack Ms. Alhathloul's iPhone, surveil her movements, and exfiltrate her confidential communications for use against her by the security services of the United Arab Emirates ("UAE"). These actions by Defendants led to Ms. Alhathloul's arbitrary arrest by the UAE's security services and rendition to Saudi Arabia, where she was detained, imprisoned, and tortured. As a result of Defendants' actions, Ms. Alhathloul continues to suffer violations of her fundamental human rights, including severe restrictions on her freedom of movement.

2. The acts committed by Defendants against Ms. Alhathloul are inextricably linked to the United States. Defendants carried out these actions using sophisticated cyber-technology developed in the United States and obtained from U.S. companies, and used this technology to target and breach Apple's computer servers located in the United States in order to infect Ms. Alhathloul's phone with malware.

3. Defendants Baier, Adams, and Gericke entered into a Deferred Prosecution Agreement with the U.S. Department of Justice in which they acknowledged and agreed to the filing of a two-count criminal Information in the United States District Court for the District of Columbia charging them with: (1) knowingly and willfully conspiring, in violation of 18 U.S.C. § 371, to violate the Arms Export Control Act ("AECA") and the International Traffic in Arms Regulations ("ITAR"); and (2) knowingly conspiring, in violation of 18 U.S.C. § 371, to commit access device fraud, and computer fraud and abuse, in violation of 18 U.S.C. §§ 1029 and 1030. As part of the Deferred Prosecution Agreement, Defendants Baier, Adams, and Gericke admitted to the conduct described in a written Factual Statement filed with the Court. Attached as Exhibit A is the Deferred Prosecution Agreement and corresponding Factual Statement, which were filed in the U.S. District Court for the District of Columbia, Case No. 1:21-cr-00577, Dkt. 4.

PARTIES

4. Plaintiff Loujain Alhathloul is a human rights defender, activist, and prominent leader in the movement to advance the rights of women and girls in her home country of Saudi Arabia. She is the recipient of numerous prestigious awards recognizing her human rights work, including the Council of Europe's 2020 Václav Havel Human Rights Award, the 2020 Sergei Magnitsky Human Rights Award, and the 2019 PEN America/Barbey Freedom to Write Award.

Ms. Alhathloul was nominated for the 2019 and 2020 Nobel Peace Prize, including by members of the United States Congress, and has also received honorary citizenship from the city of Paris.

5. On September 21, 2021, the National Constitution Center awarded Ms. Alhathloul its annual Liberty Medal for her "courage and conviction in exercising the fundamental rights of freedom of speech, nonviolent resistance, and peaceful dissent."

6. Defendant DarkMatter is an Emirati company. Beginning in or about late 2015 or early 2016, DarkMatter operated a cyber-surveillance program known as Project Raven (also known as the Development Research Exploitation and Analysis Department, or "Project DREAD"). Through Project Raven, Defendant hacked Ms. Alhathloul's iPhone, surveilled her movements, and exfiltrated her confidential communications to the UAE's security services.

7. Shortly after its inception in 2015, DarkMatter began marketing its cyber-security services to U.S. companies. For instance, DarkMatter regularly participated in, and advertised its services at, the cyber-security conference Black Hat in 2016, 2017, 2018, and 2019, hosted in Las Vegas, Nevada.

8. Defendant Marc Baier is a citizen of the United States. On information and belief, Defendant Baier is domiciled in the UAE. Defendant Baier held executive positions at DarkMatter from or about January 2016 until or about November 2019. Among other positions, Defendant Baier was lead manager of DarkMatter's Computer Network Exploitation operations and a manager of Project Raven. On or about September 7, 2021, Defendant Baier entered into a Deferred Prosecution Agreement with the U.S. Department of Justice involving criminal violations of the AECA, ITAR, Fraud and related activity in connection with access devices, and the Computer Fraud and Abuse Act ("CFAA"). As part of that Deferred Prosecution Agreement,

Defendant Baier agreed and stipulated that the information contained in a 24-page Factual Statement filed with the Court is true and accurate and that the Factual Statement correctly describes the facts and events described therein.

9. Defendant Daniel Gericke was a citizen of the United States until February 2017. On information and belief, Defendant Gericke is domiciled in Singapore. Beginning in or about October 2015, Defendant Gericke served as a manager of DarkMatter's Computer Network Exploitation operations. Between or about January 2016 and late 2018, Defendant Gericke held senior positions at DarkMatter, including managing and supporting its Computer Network Exploitation operations for Project Raven. On or about September 7, 2021, Defendant Gericke entered into a Deferred Prosecution Agreement with the U.S. Department of Justice involving criminal violations of the AECA, ITAR, Fraud and related activity in connection with access devices, and the CFAA. As part of that Deferred Prosecution Agreement, Defendant Gericke agreed and stipulated that the information contained in a 24-page Factual Statement filed with the Court is true and accurate and that the Factual Statement correctly describes the facts and events described therein.

10. Defendant Ryan Adams is a citizen and resident of the United States. Defendant Adams was employed by DarkMatter from approximately January 2016 until November 2019, and at times served as DarkMatter's Director of Cyber Operations. In this position, Defendant Adams was responsible for briefing UAE officials on the implementation of Computer Network Exploitation operations against approved UAE targets, and developing and integrating Computer Network Exploitation tools, to advance the goals of Project Raven. On or about September 7, 2021, Defendant Adams entered into a Deferred Prosecution Agreement with the U.S.

Department of Justice involving criminal violations of the AECA, ITAR, Fraud and related activity in connection with access devices, and the CFAA. As part of that Deferred Prosecution Agreement, Defendant Adams agreed and stipulated that the information contained in a 24-page Factual Statement filed with the Court is true and accurate and that the Factual Statement correctly describes the facts and events described therein.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because the action arises under the CFAA, Pub. L. No. 99-474, 100 Stat. 1213 (Oct. 16, 1986) (*codified as amended at* 18 U.S.C. § 1030) and the Alien Tort Statute, 28 U.S.C. § 1350.

12. This Court has personal jurisdiction over Defendants DarkMatter, Baier, Adams and Gericke pursuant to Fed. R. Civ. P. 4(k)(2) because the claims arise under federal law, these Defendants are not subject to jurisdiction in any state's courts of general jurisdiction, and exercising jurisdiction is consistent with the Constitution and United States law.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(3) because there is no judicial district where this action may be brought pursuant to 28 U.S.C. § 1391(b)(1) or 28 U.S.C. § 1391(b)(2), and all Defendants are subject to the Court's personal jurisdiction.

STATEMENT OF FACTS

A. Plaintiff Alhathloul's Promotion of Women's Rights in Saudi Arabia.

14. Women and girls are subject to extreme forms of repression in Saudi Arabia.

15. The U.S. Department of State 2020 Country Report on Human Rights Practices in Saudi Arabia reported that women suffer violence and discrimination. The State Department reported that "[s]ignificant human rights issues" in Saudi Arabia "included [...] violence and

discrimination against women," and that "women continued to face discrimination under law and custom."

16. Ms. Alhathloul's public advocacy on behalf of women and girls in Saudi Arabia began in 2013 when she was a student at the University of British Columbia, where she participated in social media campaigns in support of the Saudi women's rights movement. Ms. Alhathloul rose to prominence by launching a campaign to give women the right to drive, which women in Saudi Arabia were forbidden from doing until June 2018.

17. Reflecting Saudi Arabia's opposition to allowing women to drive, Saudi Crown Prince Mohammed bin Salman said in an interview in 2016 that "Saudi Arabia is not ready for women drivers." Saudi Arabia opposed Ms. Alhathloul's campaign and attempted to block its website in Saudi Arabia.

18. By carrying out her activities under her own name rather than a pseudonym, Ms. Alhathloul became the public face of Saudi Arabia's women's rights movement. For example, *NBC News* described Ms. Alhathloul as "one of Saudi Arabia's most prominent women's rights activists." When women finally received the right to drive, the *Washington Post* described this as "the culmination of a decades-long struggle by a group of Saudi feminists who suffered imprisonment, harassment, and other hardships as they campaigned for that simple right" and quoted Ms. Alhathloul's account of how "my attempt was seen as a direct challenge against the government."

19. Ms. Alhathloul's advocacy risked her personal safety and public reputation. Among other things, Ms. Alhathloul has been the subject of defamatory public campaigns

casting her as a traitor to Saudi Arabia; arbitrarily arrested by the UAE and Saudi Arabia; and subjected to human rights violations at the hands of those regimes.

20. Ms. Alhathloul was arrested for the first time in 2014 while attempting to drive across the border from the UAE—where she had a valid driver's license—to Saudi Arabia. Ms. Alhathloul publicly announced her intention to drive across the border and streamed herself doing so. Ms. Alhathloul was stopped at the border by Saudi officials and taken by the police to a detention facility where she was imprisoned for 73 days.

21. Undeterred by her arbitrary arrest and incarceration, Ms. Alhathloul continued to advocate on behalf of Saudi women and girls. Among other things, Ms. Alhathloul broadened her campaign to include ending the male guardianship system in Saudi Arabia, which required women and girls to obtain permission from a male guardian—such as a father, brother, or husband—to make basic life-decisions, including the right to work, travel, apply for higher education, and receive medical services. Ms. Alhathloul was the main voice in the movements "Together We Stand to End Male Guardianship of Women" and "Women Demand the Overthrow of Guardianship," which raised awareness and shared information online.

22. In 2016, Ms. Alhathloul helped to organize a petition to Saudi Arabia's King Salman with more than 14,000 signatures calling for the end of male guardianship. The wave of activism around this issue in 2016 was described by a Human Rights Watch researcher as "incredible and unprecedented."

23. Ms. Alhathloul's advocacy garnered significant international attention from journalists and non-governmental organizations ("NGOs") in the United States.

24. Throughout 2016 and 2017, Ms. Alhathloul worked closely with several U.S. journalists and U.S.-based NGOs, including Human Rights Watch, and other NGOs with a large presence in the United States, including Amnesty International, to broadcast her campaign for women's rights to a U.S audience.

25. In October 2016, *The New York Times* featured Ms. Alhathloul in a *Times Documentary* profiling prominent Saudi women. The documentary allowed Ms. Alhathloul to tell the story of her arrest in 2014 for attempting to drive into Saudi Arabia, and she spoke candidly to *The New York Times* about the inequities facing Saudi women and girls.

26. Throughout 2016, Ms. Alhathloul worked with researchers from Human Rights Watch, an NGO headquartered in New York City, and contributed research for their report—*Boxed In: Women and Saudi Arabia's Male Guardianship System*—which called for the end of male guardianship in Saudi Arabia. In connection with this report, Ms. Alhathloul frequently communicated with Human Rights Watch researchers located in the United States.

27. Saudi Arabia opposed Ms. Alhathloul's campaign for women's rights. For instance, Saudi Arabia's most senior cleric declared her campaign to be "a crime against the religion of Islam" and an "existential threat to Saudi society."

28. In November 2017, Ms. Alhathloul traveled to the United States to speak at an event hosted by the Arab Gulf States Institute in Washington called "Driving Forward: Women in the Gulf Assess a Changing Landscape." Ms. Alhathloul spoke about her experience advocating for women and girls in Saudi Arabia and how the recent changes in her country were dependent on "one man's will."

29. In February 2018, Ms. Alhathloul attended a meeting in Geneva, Switzerland of the United Nations Committee on the Elimination of Discrimination against Women to brief the Committee on the status of women's rights in Saudi Arabia. Ms. Alhathloul responded in real time on Twitter to the Saudi delegation's response to the Committee's questions and publicly shared her views online after the meeting.

30. On March 12, 2018, Ms. Alhathloul attempted to travel out of the UAE. Ms. Alhathloul's destination was Tunis, Tunisia, where she intended to participate in a regional consultation forum on internet universality indicators organized by the United Nations Educational, Scientific and Cultural Organization. However, Ms. Alhathloul was stopped at the airport in Abu Dhabi, taken to a room, and informed that she could not leave the UAE unless she was traveling to Saudi Arabia.

31. On March 13, 2018, Ms. Alhathloul was again arrested when she was arbitrarily detained by the UAE's security services and rendered to Saudi Arabia, as described further in paragraphs 156–171.

32. On or about May 15, 2018, after being placed under a travel ban, Saudi security officers raided Ms. Alhathloul's family home in Riyadh, arrested her, and transported her to multiple prisons. On or about May 21, 2018, Saudi security officers transferred Ms. Alhathloul to a secret prison in Jeddah, where she was interrogated and subjected to electric shocks, flogging, and threats to rape, sexually assault, and kill her.

33. In July 2021, Human Rights Watch reported "[n]ew evidence alleging Saudi Arabia's brutal torture of women's rights advocates and other high-profile detainees." The report highlighted the torture of women's rights activists detained "in early 2018, including with

electronic shocks, beatings, whippings, and sexual harassment" and documented accounts from prison guards describing "incidents in which they allege that detainees, including the prominent women's right activist Loujain al-Hathloul" suffered "torture and other ill-treatment."

34. Following her 2018 arrest, Saudi Arabia held Ms. Alhathloul without charges or trial for 10 months. The U.S. Department of State 2020 Country Report on Human Rights Practices in Saudi Arabia reported that Ms. Alhathloul was subsequently tried alongside other women activists, "all of whom remained detained and faced charges related to their human rights work and contact with international organizations, foreign media, and other activists."

35. *The New York Times* reported on the widespread international condemnation of the trial as a "sham" aimed at silencing advocacy on behalf of Saudi Arabia's women and girls. Amnesty International reported, "By failing to quash Loujain al-Hathloul's conviction, the Saudi Arabian authorities have clearly demonstrated that they consider peaceful activism a crime and consider activists to be traitors or spies."

B. The UAE and Saudi Arabia's Persecution of Perceived Dissidents.

36. The UAE and Saudi Arabia are both authoritarian, absolutist monarchies. Both persecute and cooperate in the persecution of their respective perceived dissidents.

37. The UAE targets human rights defenders and perceived dissidents through a variety of means, including digital hacking, travel bans, intimidation and harassment of their relatives, arbitrary arrest and detention, torture, and forced disappearances.

38. Human Rights Watch's World Report in 2019 reported that:

> UAE authorities have launched a sustained assault on freedom of expression and association since 2011. The UAE arbitrarily detains and forcibly disappears individuals who criticize the authorities within the UAE's borders. UAE residents who have spoken about human rights issues are at serious risk of arbitrary

> detention, imprisonment, and torture. Many are serving long prison terms or have left the country under pressure.

39. The U.S. Department of State 2020 Country Report on Human Rights Practices in the UAE reported:

> Significant human rights issues included: torture in detention; arbitrary arrest and detention, including incommunicado detention, by government agents; political prisoners; government interference with privacy rights; undue restrictions on free expression and the press, including criminalization of libel, censorship, and Internet site blocking.

40. The State Department further reported:

> Authorities treated prisoners arrested for political or security reasons differently from other prisoners, including placing them in separate sections of a prison. The State Security Department handled these cases and, in some instances, held prisoners and detainees in separate undisclosed locations for extended periods prior to their transfer to a regular prison.

41. In 2013, the UAE subjected 94 government critics and reform activists to a mass trial (known as the "UAE-94" case). The trial resulted in the conviction of 69 people (eight in absentia) receiving sentences as long as 15 years.

42. Amnesty International's 2020 report on the UAE reported:

> Emirati authorities continued to ban political opposition and to detain prisoners for such opposition. Scores of Emiratis continued to serve prison sentences in the UAE-94 case, a mass trial of 94 defendants that concluded in 2013 with 69 convicted on charges of seeking to change the system of government.

43. The United Nations Working Group on Enforced or Involuntary Disappearances determined that since 2011 the UAE has arbitrarily detained critics in violation of international law. In June 2020, the Working Group issued a report entitled *Opinion No. 33/2020 concerning Loujain Alhathloul (United Arab Emirates and Saudi Arabia)*, which concluded:

> Ms. Alhathloul's political views and convictions are clearly at the centre of the present case and that the authorities have displayed an attitude towards her that can only be characterized as discriminatory. Indeed, her human rights advocacy appears to be the sole reason for her forced transfer and detention.

44. The Working Group further concluded:

> Ms. Alhathloul's deprivation of liberty constitutes a violation of articles 2 and 7 of the Universal Declaration of Human Rights on the grounds of discrimination based on political views, gender and her status as a human rights defender.

45. In 2011, the UAE cracked down on perceived political opponents by taking over or dissolving civil society organizations, including professional organizations, such as the Teacher's Association and the Jurists' Association, after those organizations called for democratic reforms. The UAE also arrested advocates for reform, including Ahmed Mansoor, a prominent blogger and human rights advocate, and prevented peaceful demonstrations. Mr. Monsoor was held by UAE authorities for approximately six months, placed on a travel ban, and subjected to attempts to hack his personal devices to monitor his communications.

46. In 2017, the UAE re-arrested Mr. Mansoor for his ongoing efforts to draw attention to human rights violations across the Middle East. He was convicted and sentenced to ten years in prison based, in part, on the hacking of email exchanges going back to 2011 as well as encrypted WhatsApp messages between himself and representatives of Human Rights Watch, Amnesty International, and the Gulf Centre for Human Rights. Since 2018, the UAE has kept Mr. Mansoor in indefinite solitary confinement. In a communication addressed to the United Nations Human Rights Council, the Vice-Chair of the U.N. Working Group on Arbitrary Detention, the U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the U.N. Special Rapporteur on the situation of human rights

defenders, and the U.N. Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment expressed "grave[] concern[]" that Mr. Mansoor is currently held in conditions that violate international human rights.

C. The UAE and Saudi Arabia's Cooperation in Persecuting Perceived Dissidents.

47. Saudi Arabia and the UAE maintain close economic, political, military, and security ties. In 2011, public protests known as the "Arab Spring" ignited across the Middle East and North Africa demanding democratic reform and expressing discontent over economic conditions, government policies and corruption. In response to the Arab Spring, the UAE and Saudi Arabia jointly targeted individuals who peacefully expressed views that questioned or challenged their respective autocratic regimes, including women's rights advocates, human rights activists, lawyers, journalists, and academics.

48. In order to advance their mutual goals, the UAE detains and/or renders to Saudi Arabia individuals present in the UAE who promote human rights in Saudi Arabia. In 2015, for example, plain-clothed officers from the UAE's security services arrested Amina al-Abdouli, a former teacher, for criticizing Saudi Arabia and for expressing support for the Arab Spring in social media posts. After serving seven months in detention, during which Ms. al-Abdouli was frequently in solitary confinement, beaten (resulting in vision loss in her left eye) and subjected to other forms of torture, including sleep deprivation, she was charged and convicted of endangering the UAE's relations with Saudi Arabia. Ms. al-Abdouli remains imprisoned in the UAE. The charges against her included "inciting hatred" against the State and disturbing public order, undermining the reputation of State institutions, and publishing false information to endanger the State's relations with its allies. In an official communication addressed to the UAE

authorities, three U.N. Special Rapporteurs—the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health; the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; and the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment—raised concerns about her incommunicado detention, forced confession, and torture by UAE authorities. The U.N. Special Rapporteurs requested clarification on the charges against her and an explanation of how they are consistent with the UAE's international human rights obligations.

49. The U.S. Department of State 2020 Country Report on Human Rights Practices in Saudi Arabia reported that human rights organizations, the U.N., and independent third parties have expressed concern over reports of torture and severe mistreatment of women detainees, including activists and human rights advocates, by law enforcement officers. The State Department cited "[c]redible reporting by advocacy groups and press suggest[ing] authorities detained persons for peaceful activism or political opposition, including nonviolent religious figures, women's rights defenders, and human rights activists." The State Department also specifically mentioned Ms. Alhathloul's detention as an example of these ongoing abuses:

> [T]he Riyadh Criminal Court resumed trials against 11 women activists, including several arrested in 2018. Among them were [...] Loujain al-Hathloul–all of whom remained detained and faced charges related to their human rights work and contact with international organizations, foreign media, and other activists. The women were accused of violating the cybercrimes law, which prohibits production of materials that harm public order, religious values, or public morals, and carries penalties of up to five years in prison and a fine of up to three million riyals ($800,000). [...] On August 26, media reported authorities severed contact between some detainees and their families, including Loujain al-Hathloul[.]

50. In 2013, the UAE and Saudi Arabia entered into an agreement, known as the First Riyadh Agreement, under which they committed to not "harbor or naturalize any citizen" of the other who has engaged in "activity which opposes his country's regimes." In 2014, the UAE and Saudi Arabia entered in a further agreement, known as the Third Riyadh Agreement, under which they agreed that their respective intelligence chiefs would take steps to implement the First Riyadh Agreement. These steps included reporting regularly to the countries' leaders and taking measures "they deem necessary to protect the security and stability of their countries."

51. The UAE and Saudi Arabia cooperate in the persecution of their respective perceived dissidents. This cooperation includes, *inter alia*, the sharing of information, security-related cooperation, and the rendition of perceived dissidents.

52. In 2021, Freedom House, in a report entitled *Saudi Arabia: Transnational Repression Case Study*, reported on the rendition by the UAE to Saudi Arabia of Saudi nationals. The report stated that "Freedom House found renditions of Saudi nationals from [...] UAE," demonstrating "clear cooperation on the part of the host states [...] which, when combined with known security agreements among" neighboring countries, "illuminates the region's institutionalized channels of transnational repression." The report also noted that "informal and personal cooperation occurs beyond what is specified in formal security agreements."

53. The Freedom House report, in particular, found this "cooperation" between the UAE and Saudi Arabia:

> resulted in clear violations of human rights and international law. In May 2018, Loujain al-Hathloul, a prominent women's rights activist, was arrested by Abu Dhabi police while attending university in the UAE. In what was effectively a kidnapping, al-Hathloul was immediately placed on a Saudi private jet bound for Saudi Arabia; she was then issued a travel ban, and was arrested that July.

54. Similarly, the June 2020 report by the U.N. Working Group on Enforced or Involuntary Disappearances concluded:

> [T]he Government of Saudi Arabia is responsible for its action in the deprivation of liberty of Ms. Alhathloul in Saudi Arabia, as well as jointly responsible with the Government of the United Arab Emirates for the arrest, detention and forcible transfer of Ms. Alhathloul from the United Arab Emirates.

D. The UAE's Use of U.S. Corporations to Target Perceived Dissidents.

55. In order to carry out its campaign of targeting and persecuting perceived dissidents, including human rights activists, the UAE has developed advanced cyber-surveillance programs, including with the assistance of U.S. corporations and U.S. technology.

56. Beginning in or about 2008, the UAE sought out U.S. corporations to build a cyber-surveillance program known as Project Raven, the purpose of which was, *inter alia*, to target and hack perceived dissidents from the UAE and Saudi Arabia, including human rights activists.

57. In or about 2009, CyberPoint International LLC ("CyberPoint"), a U.S.-based corporation organized under the laws of Maryland, became the UAE's primary contractor on Project Raven. In developing Project Raven, CyberPoint utilized U.S. citizens recruited in the United States, including from the National Security Agency and other parts of the U.S. Intelligence Community, and transferred cyber-surveillance technology and/or techniques developed in the United States.

58. On information and belief, under CyberPoint, Project Raven employed approximately 40 U.S. personnel and had an estimated annual budget of $34 million.

59. Because CyberPoint's cyber-surveillance work for the UAE involved the export of defense articles and/or defense services covered by ITAR, promulgated by the U.S. Department of State, CyberPoint was required to obtain appropriate export licenses, including licenses from the U.S. Department of State's Directorate of Defense Trade Controls and to otherwise comply with applicable U.S. laws and regulations. CyberPoint employees who worked on Project Raven were only permitted by law to operate subject to and in compliance with those licenses and any associated Technical Assistance Agreements, and in compliance with other applicable U.S. laws and regulations.

60. The licenses permitted CyberPoint to provide defensive cybersecurity services to the UAE. The licenses did not permit CyberPoint to engage in offensive operations, such as targeting individuals for hacking or carrying out cyberattacks.

61. The terms of CyberPoint's licenses prohibited the targeting of U.S.-based servers or U.S. Persons (*i.e.*, U.S. citizens, permanent resident aliens, U.S. companies or entities, or other persons in the United States). The licenses also prohibited the re-export or re-transfer of goods, services, information and data to third parties without the consent of the U.S. government.

62. Between 2012 and 2015, Defendant Baier, a former member of the U.S. Intelligence Community, worked for CyberPoint, including as General Manager of Middle East and North Africa programs. Defendant Baier led CyberPoint's involvement in Project Raven and reported to CyberPoint's Maryland-based headquarters, including on issues of compliance with the U.S. Department of State licenses. Defendant Baier facilitated the transition of dozens of other U.S. persons to work on Project Raven to support the UAE's cyber-operations.

63. Defendant Gericke, a former member of the U.S. military, worked at CyberPoint between 2013 and December 2015 as a project leader in connection with cyber services.

64. Defendant Adams, a former member of the U.S. Air Force, served as senior software engineer for certain cyber services for CyberPoint from 2010 to 2014, and mission director and manager from 2014 to 2015.

E. The UAE Utilized Project Raven and U.S. Contractors to Target Human Rights Activists as Part of Its Campaign of Persecution.

65. While working for CyberPoint, Defendants Baier, Adams, and Gericke developed and operated Project Raven to target and hack individuals and organizations designated by the UAE, including human rights activists, journalists, academics, and other perceived dissidents.

66. On information and belief, Defendants Baier and Adams provided CyberPoint operatives working on Project Raven with information to use as a cover story for obscuring the purpose of Project Raven. For example, the "Purple briefing" given to new operatives characterized Project Raven as a defensive mission to protect the UAE from cyberattacks. However, the actual purpose of Project Raven was described in the "Black briefing," which disclosed that Project Raven was used to target and hack individuals as part of the offensive operational division of the UAE's National Electronic Security Authority (now called the Signals Intelligence Agency). These targets included perceived dissidents from the UAE and Saudi Arabia. The "Black briefing" made clear that the purpose of Project Raven should remain secret from the public.

67. CyberPoint operatives, including Defendants Baier and Adams, met regularly with the UAE's National Electronic Security Authority, which designated targets for Project Raven. Many of the targets were perceived dissidents from the UAE and Saudi Arabia.

68. Upon receipt of the target designations, Defendants Baier and Adams relayed the list of targets to other CyberPoint operatives who identified cybersecurity vulnerabilities in the selected targets and created and utilized hacking tools to carry out hacks on the targets.

69. Beginning in 2015, press reports revealed the connection between the UAE and CyberPoint. Specifically, reporting showed that CyberPoint began providing offensive cybersecurity tools to the UAE as early as 2011 through an Italian company known as the Hacking Team. The Hacking Team partnered with CyberPoint, and Defendant Baier served as the principal point of contact between the two companies. The reporting showed that CyberPoint's technology allowed UAE officials to spy on pro-democracy and human rights.

70. On information and belief, Defendants Baier and Adams knew that the targets designated by the UAE's National Electronic Security Authority included perceived dissidents of the UAE and Saudi Arabia, including human rights activists.

71. On information and belief, once the UAE's National Electronic Security Authority designated a target for CyberPoint, CyberPoint implemented the following protocol:

a. First, CyberPoint assigned the targeting division of Project Raven to surveil the target through the target's public online accounts and social media profiles. This involved, *inter alia*, seeking to identify cyber security vulnerabilities of the target that could be exploited to gain access to the target's private communications. Project Raven operatives also attempted to identify the target's friends, relatives, and associates so that these individuals could be surveilled as well.

b. Second, Project Raven's targeting division worked with the Project Raven developer division to build software for deployment in computer attacks against the target's devices and/or accounts.

c. Third, the Project Raven Initial Access Development group provided the Operations team with hacking tools designed to breach the target.

d. Fourth, the Operations team launched hacking missions against the target. Once the hacking was executed, the Operations team stole data and installed malicious software on the target's systems without their consent to maintain access and continue to surveil and exfiltrate data, including emails, photos, text messages, the target's location, and other private information.

72. While employed at CyberPoint, Defendants Baier, Adams, and Gericke oversaw Project Raven's use of U.S. technology and/or knowhow, including through the provision of defense services covered by ITAR, to carry out hacking protocols against targets identified by UAE officials.

F. Project Raven's Targeting of Perceived Dissidents, Including Human Rights Activists, Continued Under DarkMatter.

73. Beginning in or about December 2015 through February 2016, the UAE transitioned cyber services under Project Raven from CyberPoint to DarkMatter. As part of this effort, key Project Raven personnel—including Defendants Baier, Adams, and Gericke—transitioned from CyberPoint to DarkMatter.

74. During the transition, CyberPoint's legal counsel informed Defendants Baier, Adams, and Gericke that continuing to provide services to the UAE required licenses from the

Department of State because Defendants Baier, Adams, and Gericke, after leaving CyberPoint, would no longer be covered by CyberPoint's licenses.

75. Effective on or about December 31, 2015, CyberPoint terminated Defendants Baier, Adams, and Gericke. On or about that date, Defendants Baier, Adams, and Gericke, became employees of DarkMatter. Defendants Baier, Adams, and Gericke did not seek or obtain licenses from the Department of State allowing them to continue providing services to the UAE.

76. Between about January 2016 and November 2019, Defendant Baier served as the senior U.S. executive of DarkMatter and lead manager for U.S. employees of DarkMatter. Defendant Baier was responsible for overseeing DarkMatter's product acquisition and supervising DarkMatter's cyber operations, including the exploitation of electronic devices and online accounts, collection of exfiltrated information, and development of cyber-hacking tools, including for Project Raven.

77. Between about January 2016 and November 2019, Defendant Adams held various positions at DarkMatter, including serving as Director of Cyber Operations from January 2016 until or about October 2016.

78. In or about January 2016, Defendant Gericke joined DarkMatter as a supervisor of Cyber Intelligence-Operations. In or about December 2016, DarkMatter promoted Defendant Gericke to lead teams within DarkMatter's Cyber Intelligence-Operations. From about October 2017 until January 2018, Defendant Gericke served as Program Manager of DarkMatter and supervised the development of Computer Network Exploitation tools and collection.

79. With the assistance of Defendants Baier, Adams, and Gericke, DarkMatter adopted the hacking protocols developed under CyberPoint for Project Raven.

80. The hacking protocols developed under CyberPoint allowed DarkMatter to gain unauthorized access to protected computers, including computers in the United States, and thereby acquire data for the UAE's intelligence gathering efforts.

81. At least one of the hacking systems developed and deployed by Defendants Baier, Adams, and Gericke under DarkMatter for Project Raven was an ITAR-controlled defense article.

82. Defendants Baier, Adams, and Gericke did not obtain the required authorization from the U.S. government to provide defense services to foreign persons in connection with any such articles.

83. Under DarkMatter, Project Raven continued to target perceived dissidents of the UAE and Saudi Arabia, including human rights activists, journalists, academics, and other government critics. For example, in 2016, Project Raven hacked Ahmed Mansoor, the prominent Emirati activist who the UAE had previously targeted for persecution, and assigned him the code name "Egret." Based in part on intercepted communications between Mr. Mansoor and an international human rights organization, the UAE tried and convicted Mr. Mansoor in a secret trial in 2017 for purportedly publishing "false" information to damage the UAE's reputation abroad and portraying the UAE as lawless.

84. The persecution of Mr. Mansoor drew widespread international condemnation. In March 2017, multiple U.N. Special Rapporteurs whose mandates focus on human rights characterized the event as "a direct attack on the legitimate work of human rights defenders in the UAE." Similarly, Human Rights Watch concluded that "[e]very UAE state institution involved in Mansoor's conviction, persecution, and extrajudicial punishment shares

responsibility for the grave abuses that violate his rights under both UAE laws and international human rights law."

85. By June 2017, Project Raven had hacked into the mobile device belonging to Mr. Mansoor's wife, Nadia, and assigned her the code name "Purple Egret."

86. In 2017, Project Raven also targeted and hacked the iPhone of Tawakkol Karman, a Yemeni human rights activist who received the Nobel Peace Prize in 2011 for her activism on behalf of women's rights and democracy.

G. Defendants Acquired U.S. Technology to Carry Out Hacks on Apple Devices in Furtherance of Project Raven's Objectives.

87. Under the direction of Defendants Baier, Adams, and Gericke, DarkMatter acquired new "exploits"—that is, computer code that takes advantage of a vulnerability in an application in order to realize some functionality, such as the installation of malware, not foreseen or intended by the application's designer. These exploits included ones that took advantage of vulnerabilities in the Apple operating system software ("iOS"), including Apple's Messages application ("Messages app"), in order to hack Apple devices.

88. The exploits acquired by Defendants included "zero-click" exploits, which run without the exploit's target taking any action, such as clicking on a link, navigating to a website, or installing an app.

89. The purpose of these "zero-click" exploits was to install malware on the devices of its target without the target's awareness or authorization. "Malware" is code that is unwanted by the intended user of the application and may perform any of a variety of functions, including allowing access to, collection, deletion, or modification of data on the device.

90. The "zero-click" exploit is sent by an attacker to the target's device. "Attacker" refers to the entity that uses an exploit or malware on a target.

91. The iOS exploits acquired and utilized by Defendants allowed Project Raven operatives to hack into the iPhones of hundreds of targets in order to obtain, among other things, emails, location data, text messages, and photographs.

92. Defendants developed and repeatedly deployed an espionage platform known as "Karma," which used a "zero-click" iMessage exploit to leverage a vulnerability in the Apple Message app to install malware on the target's iPhone and exfiltrate data.

93. Defendant Baier, acting on behalf of DarkMatter, communicated with two U.S. companies to acquire two "zero-click" iMessage exploits ("Exploit 1" and "Exploit 2") in order to create Karma and upgrade Karma to overcome evolving iOS security upgrades put in place by Apple.

94. On or about May 2016, Defendant Baier, acting on behalf of DarkMatter, acquired Exploit 1 from a U.S. company.

95. DarkMatter paid approximately $750,000 for Exploit 1 by transferring funds from a bank account outside the United States to the bank account in the United States belonging to the U.S. company.

96. On information and belief, Defendant Baier, acting on behalf of DarkMatter, entered into a contract for the acquisition of Exploit 1 from the U.S. company.

97. On information and belief, Defendants Baier, Adams, and Gericke were in direct contact with the U.S. company about how to configure Exploit 1 into a hacking system for DarkMatter.

98. In September 2016, Apple patched vulnerabilities in its operating system and thereby made Exploit 1 less effective.

99. On or about October 2016, Defendant Baier, acting on behalf of DarkMatter, acquired Exploit 2, together with other computer network exploitation tools and maintenance services, from a U.S. company.

100. On information and belief and based on reporting, that company was Accuvant LABS, which was since acquired by its current owner, Optiv. *See* Patrick Howell O'Neill, *This US company sold iphone hacking tools to UAE spies*, MIT Technology Review (September 15, 2021), available at https://www.technologyreview.com/2021/09/15/1035813/us-sold-iphone-exploit-uae/.

101. DarkMatter paid approximately $1,300,000 to this U.S. company by transferring funds from a bank account outside the United States to a United States bank account belonging to the U.S. company.

102. On information and belief, Defendant Baier, acting on behalf of DarkMatter, entered into a contract with the U.S. company for the acquisition of Exploit 2 and for other computer network exploitation tools and maintenance services.

103. On information and belief, Defendants Baier, Adams, and Gericke were in direct contact with the U.S. company about how to configure Exploit 2 into a hacking system for DarkMatter.

104. Defendants Baier, Adams, and Gericke supported, directed, and supervised DarkMatter in creating the Karma hacking system that relied on the obtained exploits.

105. To enhance the effectiveness of Karma, Defendants Baier, Adams, and Gericke equipped the exploits with other U.S. technology, including anonymization services, proxy servers, and computer hardware located or built in the United States.

106. The services performed by Defendants Baier, Adams, and Gericke in connection with the Karma hacking system constituted defense services under United States Munitions List ("USML") Category XI(d), for which Defendants did not have a license to provide such ITAR-controlled defense services.

107. Among the enhancements made to the exploit, Defendants utilized a U.S. company's anonymization services and proxy servers to prevent detection and mask the true origin of transmissions from the Karma hacking system.

108. On information and belief, Defendants masked the origin of their hacking transmissions by routing their communications through U.S.-based anonymization services and other proxy servers hosted in the United States to prevent detection and attribution.

109. By enhancing Karma with other U.S.-based technology, Defendants improved the efficacy of Karma, making it successful in 90 to 95% of deployments and helping DarkMatter evade detection.

110. Defendants Baier, Adams, and Gericke recruited U.S. individuals with cyber-hacking expertise, and who possessed unique cyber-hacking knowhow developed in the United States, to work at DarkMatter and assist in the development of the Karma hacking system.

H. Defendants' Hacking Activity Utilized Servers Located in the United States.

111. A "zero-click" iMessage exploit, such as that used by Karma, necessarily targets and utilizes servers located in the United States to carry out the hack because the attacker must

transmit the exploit and malware to servers in the United States in order to infect the target's device.

112. First, the attacker registers an Apple account so that the attacker can send iMessages in the Messages app. The attacker then inputs the target's email address or telephone number linked to the target's Apple account into a custom program that sends a specifically crafted iMessage, containing an exploit and malware, to servers located in the United States to reach the target's device.

113. To send an iMessage, the attacker retrieves the recipient's encryption and routing information from Apple's identity servers. The identity servers are a group of servers on which Apple stores encryption and routing information for Messages app users (as well as other Apple-provided services). The identity servers are located in the United States.

114. Next, the attacker encrypts the iMessage using the information from the identity servers and sends the iMessage to the Apple Push Notification Service. The Apple Push Notification Service is a group of servers in which Apple receives, temporarily stores, and sends data to Apple device users, including Messages app users. The Apple Push Notification Service is located in the United States.

115. The Apple Push Notification Service receives, stores, and delivers the iMessage to each of the recipient's Apple devices with the Messages app. The Apple Push Notification Service deletes its copy of the iMessage upon delivery or stores it for up to 30 days if any of the recipient's devices are offline.

116. Finally, if the iMessage has an attachment or is otherwise large, which is the case with malware payloads, the attachment is encrypted and uploaded to Apple's storage servers,

colloquially called iCloud. iCloud is a group of servers, including several in the United States, in which Apple receives, stores, and sends data to Apple device users.

117. As a result, to transmit a "zero-click" iOS exploit to the target, the attacker interacts with Apple's U.S.-based servers several times: the attacker retrieves information from identity servers; the iMessage is stored on Apple Push Notification Service temporarily or for up to 30 days; the Apple Push Notification Service sends the iMessage to the recipient device(s); and the iMessage attachment, the malware payload, is stored on iCloud.

118. To connect to the Apple Push Notification Service, the sender's device contacts a server located at api.push.apple.com, which is a human-readable domain name for a server or group of servers connected to the internet. Domain names can be converted, or resolved, to Internet Protocol (IP) addresses, which computers connected to the internet (including servers) use to route information to each other. Online domain name system servers resolve domain names: that is, they convert domain names into IP addresses. A computer can generally be located geographically by looking up its IP address in an online database of location information, with high accuracy at the country level. Online domain name system servers provide the following IP addresses for the Apple Push Notification Service: 17.188.182.137, 17.188.180.78, 17.188.183.10, 17.188.182.206, 17.188.182.207, 17.188.182.204, 17.188.180.79, 17.188.182.10.

119. Online domain name system servers provide the following IP addresses for the identity servers: 17.32.194.37, 17.32.194.6.

120. At the time of the hack of Ms. Alhathloul's phone, these IP addresses were located in the United States. Consequently, sending an iMessage required the sender and recipient of an iMessage exploit to interact with Apple's servers in the United States.

121. Since the identity servers and the Apple Push Notification Service are located in the United States, an attacker using Karma necessarily had to retrieve the target's encryption and routing information from, and send the exploit and malware through, Apple servers located in the United States in order to hack the target's phone.

122. After the attacker uses the identity servers and the Apple Push Notification Service to send the malware-containing iMessage to the target, and the malware is uploaded to iCloud, the Messages app on the target's iPhone receives and processes the attacker's iMessage. The Messages app automatically processes all messages it receives and retrieves their attachments from iCloud without any action being required by the target. The act of processing the "zero-click" exploit embedded in the iMessage or its attachment activates the exploit, and the exploit uses a vulnerability in the Messages app to interrupt the app and execute the exploit's code. The Messages app may be interrupted before it displays a notification to the target (*i.e.*, "New message from ..."), so the exploit may be invisible to the target.

123. Upon execution, the exploit code installs malware on the target's iPhone. The malware can access and modify data within the Messages app, and therefore is capable of viewing all iMessages on the recipient's device.

124. To access other data, the attacker's malware must run additional stages of exploits to circumvent security and access restrictions in the iPhone's operating system. Those exploits then install additional malware. The malware can then provide the attacker access to all data on the iPhone.

125. The additional malware enables the attacker to access data on other apps, including communication services that use security features, including Telegram and WhatsApp.

Both Telegram and WhatsApp send only end-to-end-encrypted messages, such that the messages are only unencrypted and readable on the intended sender's and recipient's devices, not while in transit between them, when they are encrypted. Thus, unlike a standard telephone call, the attacker's malware cannot intercept and read messages while in transit, but it can read them on the devices.

126. The final step of the attack occurs when the malware installed on the iPhone connects to an attacker-controlled server. The malware exfiltrates data from the iPhone to the server. The attacker's server may send commands to the malware that the malware executes. The server may command the malware to collect and transfer specific data, run additional exploits, or uninstall itself to avoid future detection.

127. Devices that were compromised by Karma continuously transmit data stored on the compromised device to servers controlled by Project Raven.

128. Defendants created numerous inauthentic Apple accounts, and in doing so assented to Apple's Terms of Service, in order to access Apple servers to acquire recipients' encryption and routing information, test the effectiveness of Karma, and deploy the exploit and malware.

129. On information and belief, DarkMatter used Apple's Messages app, the Apple Push Notification Service, the identity servers, and the iCloud servers to deploy an iOS exploit and malware to Ms. Alhathloul's device, surveil her communications, and exfiltrate data to a DarkMatter controlled server.

130. In doing so, DarkMatter intentionally or recklessly transmitted malware that utilized servers located in the U.S. to carry out the hack.

131. Defendants Baier, Adams, and Gericke each possessed computer network exploitation expertise, including in the development, maintenance, deployment, and operation of hacking technology designed to obtain unauthorized access to protected computers.

132. Owing to their computer network exploitation expertise, on information and belief, Defendants Baier, Adams, and Gericke each possessed a technical understanding of how the Karma exploits functioned, including that the exploits relied on Apple's U.S.-based servers to reach a target's device.

I. As Part of Its Persecution of Perceived Dissidents, Project Raven Targeted and Hacked Plaintiff Alhathloul.

133. Public reporting by *Reuters*, based on interviews with whistleblowers who previously worked on Project Raven and an independent review of Project Raven documents, revealed that Project Raven "utilized an arsenal of cyber tools, including a cutting-edge espionage platform known as Karma, in which Raven operatives say they hacked into the iPhones of hundreds of activists." Former Project Raven operatives explained to *Reuters* that "[i]n 2016 and 2017, Karma was used to obtain photos, emails, text messages and location information from targets' iPhones."

134. Later reporting by *Reuters* revealed that Project Raven targeted and hacked Ms. Alhathloul in 2017. During the course of DarkMatter's surveillance of Ms. Alhathloul, DarkMatter assigned her the codename "Purple Sword." This hacking preceded her arrest in the UAE and rendition to Saudi Arabia.

135. On information and belief, DarkMatter operatives hacked Ms. Alhathloul's iPhone by targeting her as a recipient of the "zero-click" iOS exploit and malware.

136. On information and belief, DarkMatter's exploit and malware were received by Ms. Alhathloul's device, and relying on a flaw in Apple's iOS, installed malware on Ms. Alhathloul's iPhone.

137. On information and belief, this process executed DarkMatter's malware that remained on Ms. Alhathloul's iPhone, enabling Defendants to view the contents on her device and automatically exfiltrate data to a separate server controlled by DarkMatter.

138. DarkMatter's malware was designed to view and exfiltrate location data and data from applications on the device, such as iMessages, email, Facebook, WhatsApp, and Telegram.

139. On information and belief, this malware was designed to, and did, allow DarkMatter to monitor Ms. Alhathloul's private communications across multiple social media and communications platforms by repeatedly and continuously exfiltrating data from Ms. Alhathloul's device to a server controlled by DarkMatter.

J. Project Raven Exfiltrated Data From Ms. Alhathloul's Device While She Was Physically Present in the United States.

140. DarkMatter's hacking of Ms. Alhathloul's iPhone was part of the UAE's campaign of persecution against perceived dissidents of itself and Saudi Arabia. The hacking was intended to provide constant surveillance of Ms. Alhathloul's communications with other human rights advocates, researchers, and journalists, including U.S.-based human rights advocates, researchers, and journalists.

141. From 2016 to 2018, Ms. Alhathloul collaborated with several U.S.-based human rights advocates, researchers, and journalists to build international support for women's rights in Saudi Arabia.

142. On information and belief, the malware used by Project Raven was designed to, and did, allow DarkMatter to receive real-time location information to monitor the movements, whereabouts and communications of Ms. Alhathloul, including information about her private communications with U.S.-based human rights advocates, researchers, and journalists.

143. On November 28, 2017, and during this period of surveillance, Ms. Alhathloul flew to Washington, D.C. to attend a conference—Driving Forward: Women in the Gulf Assess a Changing Landscape"—held by the Arab Gulf States Institute in Washington ("AGSIW"). Ms. Alhathloul was one of two featured speakers at the event.

144. Ms. Alhathloul's attendance at the event was promoted on Twitter by AGSIW on November 17, 2017.

145. The next day, another Saudi women's rights advocate, Nora Abdulkarim promoted Ms. Alhathloul's attendance at the event to her thousands of Twitter followers.

146. After arriving in Washington, D.C., Ms. Alhathloul announced on Twitter that she was in the United States.

147. On November 30, 2017, Ms. Alhathloul participated in the AGSIW panel and publicly criticized the KSA government because the recent changes and advancements in her country were dependent on "one man's will."

148. Ms. Alhathloul brought her iPhone with her during her visit to the United States. From November 28, 2017 until her return to the UAE on December 2, 2017, Ms. Alhathloul used the device to communicate with friends, family, and other human rights advocates, including individuals in the United States.

149. On information and belief, the data exfiltrated from Ms. Alhathloul's device by Defendants included her private communications with U.S.-based human rights advocates, researchers, and journalists, as well as private communications she made while physically present in the United States.

150. On information and belief, and due to the continuous and ongoing hack against Ms. Alhathloul's device, Defendants exfiltrated private encrypted data from Ms. Alhathloul's device while she was physically present in the United States.

151. In doing so, Defendants thwarted the integrity and security of the iPhone that Ms. Alhathloul relied on in conducting her human rights work.

152. Ms. Alhathloul specifically chose to use an iPhone because of its reputation for enhanced security features and knowledge that it relied on servers located in the United States. Ms. Alhathloul's community of human rights advocates generally trusted the safety of iPhones and chose, for example, iPhone's FaceTime videoconferencing believing it offered one of the few safe modes of videoconference communication.

153. Following the hacking of Ms. Alhathloul's iPhone, and during the period of her continued surveillance, the UAE limited her international travel solely to Saudi Arabia, arbitrarily detained her, and forcibly rendered her to Saudi Arabia, where the torture to which she was subject was foreseeable in light of Saudi Arabia's practices in regard to perceived dissidents.

154. The hack against Ms. Alhathloul resulted in a disruption to her ongoing work with U.S.-based human rights advocates, researchers, and journalists.

155. Ms. Alhathloul did not discover that she was a victim of hacking by DarkMatter until she became aware of the reporting by *Reuters* describing DarkMatter's hack on her.

K. Following the Hacking of Her iPhone, Plaintiff Alhathloul was Forcibly Rendered by the UAE to Saudi Arabia Where She Was Tortured by the Saudi Security Services.

156. On March 12, 2018, Ms. Alhathloul presented herself at Abu Dhabi airport in order to fly to Tunis, Tunisia. At the airport, she was stopped, taken to a room and informed that she could not travel out of the UAE unless she was going to Saudi Arabia. This was the first time Ms. Alhathloul learned that she was under a travel ban in the UAE.

157. On or about March 13, 2018, Ms. Alhathloul was driving on Sheikh Zayed Bin Sultan Road in Abu Dhabi when two unmarked vehicles intercepted her. Ms. Alhathloul was ordered to stand and several men jumped out of the vehicles and surrounded her. They placed her inside a sealed section of one of the vans and handcuffed her; the windows were covered, and a camera monitored her. Ms. Alhathloul was transported to an unknown building, where she saw an "Abu Dhabi Police" logo. She was held in a monitored room without knowledge of what would happen to her. Upon Ms. Alhathloul's arrest, she was not shown a warrant or provided information about the grounds for her detention. None of the members of the security services identified themselves.

158. After approximately four hours in the detention room, the officers placed Ms. Alhathloul, blindfolded and handcuffed, in a vehicle that transported her to an airport, where she was forcibly placed on an aircraft and flown to Riyadh, Saudi Arabia.

159. On information and belief, the aircraft was owned and operated by the UAE.

160. Upon landing at the King Khalid airport in Riyadh, the members of the UAE security services who had accompanied her remained in the aircraft while Saudi officials, including a uniformed officer, entered the plane, took paperwork from the crew, and escorted

Ms. Alhathloul out. Ms. Alhathloul was then transported to and detained in Ha'er prison for two days without charge.

161. On March 15, 2018, Ms. Alhathloul was allowed to leave Ha'er prison, but the Saudi government imposed a travel ban, preventing her from leaving Saudi Arabia. As collective punishment, Ms. Alhathloul's family members were also placed on a travel ban, which remains in place to this day.

162. On or about May 15, 2018, members of the Saudi security services raided the home of Ms. Alhathloul's family and arrested her. The officers who arrested Ms. Alhathloul then raided the homes of two other women activists who were also arrested.

163. Ms. Alhathloul was taken to Al-Hayar prison in Riyadh. A few hours later, Ms. Alhathloul was transferred, with another woman detainee, to Dhahban prison in Jeddah, Saudi Arabia.

164. About six days later, Ms. Alhathloul was moved to a secret prison for interrogation where she was subjected to torture. On December 5, 2018, Ms. Alhathloul submitted a complaint of torture to the Public Prosecution and Saudi Human Rights Commission. The complaint requested that Saudi Arabia's Attorney General investigate those who tortured her in the secret prison. In a statement, the Attorney General claimed that female detainees enjoyed good treatment, without addressing Ms. Alhathloul's complaint.

165. During Ms. Alhathloul's interrogation and torture, her interrogators mentioned details regarding Ms. Alhathloul's communications that were available through unlawful access of Ms. Alhathloul's device.

166. On or about July 4, 2018, Ms. Alhathloul was transferred from the secret prison to Dhahban prison.

167. In March 2019, Ms. Alhathloul was tried by the Specialized Court of Saudi Arabia. Ms. Alhathloul's trial was condemned as a sham trial lacking in basic due process.

168. Ms. Alhathloul's charging document stated that she "was arrested after finding information of her contacting dissidents abroad and what has been found on her social media account by engaging in 'inciting activities.'" The Chair and Vice Chair of the U.N. Working Group on discrimination against women and girls described the charges against Ms. Alhathloul as "spurious" and demanded her release.

169. The charging document referenced private communications stored on Ms. Alhathloul's iPhone. These included private communications between Ms. Alhathloul and other human rights activists that had been transmitted via Telegram and WhatsApp, both end-to-end encrypted messaging services.

170. The charging document also referenced Ms. Alhathloul's participation in conferences and panels relating to Saudi women's rights, her contacts with international organizations and foreign journalists, and her communications with human rights advocates and NGOs located abroad, including in the United States.

171. On information and belief, Ms. Alhathloul's arrest and rendition by the UAE, as well as her detention and torture by Saudi Arabia, were facilitated by Project Raven's hack of her iPhone using an iOS exploit, the resulting surveillance, and the access to and sharing of information exfiltrated as a result of the hack between or among Project Raven, UAE, and Saudi Arabia.

L. Defendants Baier, Adams, and Gericke Entered into a Deferred Prosecution Agreement Concerning the Conduct Alleged in This Complaint.

172. In 2021, Defendants Baier, Gericke, and Adams entered a Deferred Prosecution Agreement with the National Security Division of the U.S. Department of Justice, and U.S. Attorney's Office for the District of Columbia arising out of their conduct while employees at CyberPoint and DarkMatter. As part of that Deferred Prosecution Agreement, Defendants Baier, Adams, and Gericke agreed and stipulated that the information contained in a 24-page Factual Statement filed with the Court is true and accurate and that the Factual Statement correctly describes the facts and events described therein.

173. The offenses covered under the Deferred Prosecution Agreement include knowingly and willfully conspiring to violate: (1) the AECA, (2) ITAR, (3) 18 U.S.C. § 1029 (Fraud and related activity in connection with access devices), and (4) 18 U.S.C. § 1030 (Computer Fraud and Abuse Act).

174. On information and belief, the Deferred Prosecution Agreement's reference to "U.S. COMPANY ONE" refers to CyberPoint; the reference to "U.A.E. CO" refers to DarkMatter; the reference to "U.S. COMPANY TWO" refers to Apple; and the reference to "MESSENGER" refers to the Apple Messages app.

M. Defendants Baier, Adams, and Gericke Entered into Consent Agreements with the U.S. Department of State Concerning the Conduct Alleged in This Complaint.

175. In July 2022, Defendants Baier, Gericke, and Adams each entered a Consent Agreement with the Directorate of Defense Trade Controls, Bureau of Political-Military Affairs of the U.S. Department of State arising out of their conduct while employees at CyberPoint and DarkMatter. As part of the Consent Agreements, the U.S. Department of State filed Proposed

Charging Letters for each individual. Each Proposed Charging Letter notified Defendants Baier, Adams, and Gericke of the U.S. Department of State's intention to institute administrative proceedings under § 38 of the Arms Export Control Act and ITAR. The Consent Agreements and Proposed Charging Letters for Defendants Baier, Adams, and Gericke are attached as Exhibit B.

176. The Proposed Charging Letters describe the Defendants' alleged violations of the Arms Export Control Act and ITAR. These violations arose out of the Defendants' unauthorized provision of defense services to the UAE in connection with Project Raven.

177. The Proposed Charging Letters describe how the actions taken by Defendants Baier, Adams, and Gericke in connection with Project Raven constituted the provision of unlicensed "defense services under USML Category XI(d) because: (a) the relevant systems were electronic systems, equipment, or software that were specially designed for intelligence purposes that collect, survey, monitor, or exploit, or analyze or produce information from the electromagnetic spectrum as described in USML Category XI(b); and (b) Respondent assisted foreign persons in the use, design, development, engineering, production, modification, testing, maintenance, processing, or operation of the relevant systems."

FIRST CLAIM FOR RELIEF
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT
(All Defendants)

178. Ms. Alhathloul re-alleges and incorporates by reference all preceding paragraphs.

179. The CFAA prohibits the unauthorized access of a protected computer.

180. The CFAA provides for a civil cause of action when the unauthorized access of a protected computer causes damage or loss, and the conduct involves (1) loss to 1 or more persons during any 1-year period of $5,000 or greater, (2) the modification or impairment, or

potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals, (3) physical injury to any person, (4) a threat to public health or safety, (5) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security, or (6) damage affecting 10 or more protected computers during any 1-year period.

181. The acts alleged herein constitute four separate violations of the CFAA by Defendants DarkMatter, Baier, Adams, and Gericke.

182. Ms. Alhathloul's mobile device is a protected computer because it is "used in or affecting interstate or foreign commerce or communication" by virtue of its connection to the internet.

183. Ms. Alhathloul suffered damage or loss due to Defendants' violations.

184. Defendants' conduct involved loss to Ms. Alhathloul aggregating at least $5,000. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I).

185. In the alternative, Defendants' conduct involved physical injury to Ms. Alhathloul. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(III).

A. Violation 1 - 18 U.S.C. § 1030(a)(2)(C)

186. Defendants intentionally, and without authorization, accessed Ms. Alhathloul's mobile device, and as a result of such conduct, obtained information from a protected computer.

187. Access to Ms. Alhathloul's mobile device was accomplished by sending an exploit and malware to the phone through Apple's U.S.-based servers. This malware remained embedded on Ms. Alhathloul's iPhone capable of viewing content on her device and exfiltrating the data to a DarkMatter server, including while she was physically present in the United States.

B. Violation 2 – 18 U.S.C. § 1030(a)(5)(A)

188. Defendants violated the CFAA by causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage without authorization, to Ms. Alhathloul's mobile device.

189. Defendants caused the transmission of an exploit to Ms. Alhathloul's device with the intention of installing malware to the device that would transmit data from her device to a DarkMatter server. This access was without authorization.

190. Defendants caused the transmission of malware to Ms. Alhathloul's mobile device by retrieving Ms. Alhathloul's encryption and routing information from Apple's U.S.-based servers and directing Apple's U.S.-based servers to transmit an iMessage containing an exploit and malware to Ms. Alhathloul's iPhone.

191. As a result, Defendants intentionally caused damage to parts of Ms. Alhathloul's iPhone by infecting it with an exploit and malware, which impaired the integrity of data on her iPhone and compromised the security systems on her device.

192. The malware routed Ms. Alhathloul's data to a separate server controlled by DarkMatter, including while she was physically present in the United States.

193. The intentionality of the damage is established by Defendants' purposeful engagement in cyber espionage.

C. Violation 3 – 18 U.S.C. § 1030(a)(5)(B)

194. Defendants violated the CFAA by intentionally accessing Ms. Alhathloul's mobile device without authorization, and as a result of such conduct, recklessly caused damage.

195. Defendants accessed the contents of parts of Ms. Alhathloul's iPhone by transmitting an iMessage exploit and malware to Ms. Alhathloul's iPhone.

196. The malware recklessly caused damage because the installation of malicious code, which impaired the integrity of data on her iPhone and compromised the security systems on her device, was a foreseeable result of directing the exploit to an individual's iPhone.

D. Violation 4 – 18 U.S.C. § 1030(a)(5)(C)

197. Defendants violated the CFAA by intentionally accessing Ms. Alhathloul's mobile device without authorization, and as a result of such conduct, caused damage and loss.

198. Defendants accessed information from Ms. Alhathloul's mobile device using embedded malware, including while she was physically present in the United States. The malware sent the data from Ms. Alhathloul's mobile device to servers controlled by DarkMatter. This allowed Defendants to obtain private information contained on Ms. Alhathloul's iPhone without authorization.

199. As a result, the Defendants caused damage to parts of Ms. Alhathloul's iPhone by impairing the integrity of data on her iPhone and compromising the security systems of the device, and caused loss.

E. Plaintiff Alhathloul Suffered Loss and Damage under the CFAA.

200. Ms. Alhathloul suffered damage to her iPhone as defined in 18 U.S.C. § 1030(e)(8) because she suffered impairment to the integrity of the data on her iPhone by virtue of the hack, including while physically present in the United States.

201. Ms. Alhathloul also suffered impairment to the security systems on her iPhone, which were essential for her to carry out her work free from persecution.

202. Ms. Alhathloul used her device to conduct her work as a human rights activist, including using the device to communicate with journalists, researchers, and other human rights advocates, many of whom were located in the United States.

203. Ms. Alhathloul suffered loss aggregating at least $5,000 in value. This loss includes costs incurred due to responding to the hack, conducting a damage assessment, and attempting to restore data.

204. For instance, Ms. Alhathloul has spent at least 100 hours responding to the hacks committed against her, including communicating with cyber-security experts about the hack, contacting individuals whose information may have been intercepted by Defendants' hack, developing new security protocols, and remaining informed about the latest threats against her digital security.

205. Due to the hack, Ms. Alhathloul has had to employ new security measures to protect the confidentiality of her communications, which has impaired her ability to carry out her human rights work.

206. In addition to these losses, Ms. Alhathloul suffered other compensatory damages as a result of the hack, as described in paragraphs 207–211.

207. Ms. Alhathloul lost access to files located on her device as a result of the hack and subsequent arrest.

208. Ms. Alhathloul entered into a business contract with TwoFour54 worth over $2,722 USD a month prior to her arrest. Due to the hack and subsequent arrest, Ms. Alhathloul's contract was cancelled.

209. Due to the hack and subsequent arrest, the vehicle Ms. Alhathloul was driving at the time of her arrest was impounded and its current whereabouts are unknown, resulting in a total loss.

210. Ms. Alhathloul suffered economic loss due the disruption to her life, schooling, and career of activism because the hack enabled the UAE and Saudi Arabia to arrest, detain, and torture Ms. Alhathloul. Ms. Alhathloul continues to suffer loss as a result of the hack and her subsequent detention.

211. Ms. Alhathloul was expected to graduate with a Master's Degree from Sorbonne University in the summer of 2018, which has been delayed four years to the summer of 2022.

212. Ms. Alhathloul suffered physical injury by reason of the hack and ongoing surveillance because it enabled and/or otherwise caused her arbitrary detention by the UAE and her rendition to and torture by Saudi Arabia.

213. Following Ms. Alhathloul's arrest, UAE officials transported her to Saudi Arabia and rendered her to the custody of Saudi Arabia. While in Saudi custody, she was held under various forms of arrest. During this period, Ms. Alhathloul was tortured, resulting in physical and emotional injuries.

214. On information and belief, information obtained through Defendants' hack in part formed the basis for Saudi Arabia's detention, charging, prosecution, and punishment of Ms. Alhathloul.

SECOND CLAIM FOR RELIEF
CONSPIRACY TO VIOLATE THE COMPUTER FRAUD AND ABUSE ACT
(All Defendants)

215. Ms. Alhathloul re-alleges and incorporates by reference all preceding paragraphs.

216. By participating together in this conduct—and with UAE officials—Defendants engaged in a conspiracy to violate the CFAA.

217. An actual or tacit agreement existed between UAE officials and Defendants DarkMatter, Baier, Adams, and Gericke to commit violations of the CFAA.

218. While employed at CyberPoint, Defendants Baier, Adams, and Gericke developed and operated Project Raven to target and hack individuals and organizations designated by the UAE.

219. As employees of CyberPoint, Defendants Baier, Adams, and Gericke reached an actual or tacit agreement with each other, and with UAE officials and DarkMatter, to transfer U.S. technology and knowhow regulated by ITAR to DarkMatter for the purpose of implementing Project Raven's hacking protocols and gaining unauthorized access to protected computers.

220. By facilitating the transfer of U.S. technology and knowhow to DarkMatter for the knowing purpose of assisting and carrying out hacks against targets of Project Raven, including against protected computers, Defendants engaged in an actual or tacit agreement to commit violations of the CFAA.

221. Defendants carried out their hacks against targets identified by UAE officials and knowingly facilitated the transfer of information collected from their hacks to UAE officials.

222. Defendants committed numerous overt acts in, and directed at, the United States in furtherance of their initial conspiracy. Defendants purchased two "zero click" exploits from U.S. companies, fashioned these exploits into the hacking system Karma, actively recruited other U.S. persons with unique cyber-hacking expertise to help commit CFAA violations, and

purchased other U.S. technology and hardware, including anonymization services and proxy servers, from U.S. companies to enhance Karma.

223. On information and belief, DarkMatter, under the supervision of Defendants Baier, Adams, and Gericke, entered into contracts with U.S. companies in furtherance of their conspiracy to commit CFAA violations.

224. Among their overt acts in furtherance of the initial conspiracy, Defendants Baier, Adams, and Gericke directed, assisted, and supervised hacks against numerous Project Raven targets identified by UAE officials, including Ms. Alhathloul.

225. Defendants are liable for the foreseeable crimes and other conduct, including the hack against Ms. Alhathloul, committed in furtherance of the initial conspiracy.

226. By reason of Defendants' conspiracy, Ms. Alhathloul suffered damage, loss, and physical injury, as described in paragraphs 200–214.

THIRD CLAIM FOR RELIEF
PERSECUTION AS A CRIME AGAINST HUMANITY UNDER THE ALIEN TORT STATUTE
(Defendants Baier, Adams, and Gericke)

227. Ms. Alhathloul re-alleges and incorporates by reference all preceding paragraphs.

228. The acts alleged herein constitute the crime against humanity of persecution on discriminatory grounds, a "tort . . . committed in violation of the laws of nations or a treaty of the United States" under the Alien Tort Statute, 28 U.S.C. § 1350. Persecution as a crime against humanity violates customary international law prohibiting crimes against humanity as reflected, expressed, defined, and codified in multilateral treaties and other international instruments, international and domestic judicial decisions, and other authorities.

229. Since at least 2011, the UAE has engaged in a widespread or systematic attack directed against a civilian population, namely perceived dissidents of the UAE and Saudi Arabia, including human rights activists, journalists, academics, and other individuals viewed as expressing opinions critical of their respective autocratic regimes. This systematic or widespread attack on this civilian population has included, *inter alia*, hacking the devices and tracking the locations of members of the persecuted group; stealing their personal information; imposing travel bans; and subjecting them to arbitrary arrests and detention, sham trials, torture, enforced disappearances, extrajudicial killings, as well as harassment and abuse of their family members.

230. As part of this widespread or systematic attack, the UAE targeted Ms. Alhathloul because of her public advocacy in opposition to the policies of the ruling regime in Saudi Arabia. In targeting Ms. Alhathloul, the UAE was aided and abetted by Defendants Baier, Adams, and Gericke, who knew of, and/or otherwise intended to participate in, the widespread or systematic attack committed by the UAE against perceived dissidents of the UAE and Saudi Arabia, including the persecution of Ms. Alhathloul.

231. Defendants Baier, Adams, and Gericke also conspired with DarkMatter and the UAE to persecute Ms. Alhathloul. An actual or tacit agreement existed between Defendants Baier, Adams, Gericke, DarkMatter, and the UAE to target perceived dissidents, including human rights activists, women's rights activists, journalists, academics. Defendants Baier, Adams, and Gericke developed, maintained, deployed and operated Project Raven to facilitate the UAE's persecution of these perceived dissidents, including Ms. Alhathloul.

232. The acts and omissions of Defendants Baier, Adams, and Gericke directly and proximately caused Ms. Alhathloul to suffer severe and ongoing physical and mental pain and suffering.

233. Ms. Alhathloul has suffered damages in an amount to be determined at trial as a result of her persecution as a crime against humanity.

234. The acts and omissions of Defendants Baier, Adams, and Gericke were deliberate, willful, intentional, wanton, malicious, and oppressive, and should be punished by an award of punitive damages in an amount to be determined at trial.

PRAYER FOR RELIEF

To the extent permitted by law, Ms. Alhathloul seeks the following relief against Defendants:

(a) Compensatory damages;

(b) Punitive damages;

(c) Injunctive relief, including an order that the Defendants cease taking any actions relating to hacking Ms. Alhathloul's devices;

(d) Reasonable attorneys' fees, costs and expenses; and,

(e) Such other and further relief as the Court may deem just and proper.

//

//

//

//

//

Jury Trial Request

Ms. Alhathloul requests a trial by jury for each claim for relief and all triable issues.

Dated: May 8, 2023

/s *Christopher E. Hart*

BOISE MATTHEWS DONEGAN LLP
Bridget M. Donegan
OSB No. 103753
805 SW Broadway, Suite 1900
Portland, OR 97205
(503) 228-0487
bridget@boisematthews.com

FOLEY HOAG LLP
Christopher E. Hart
MA BBO No. 625031
Anthony D. Mirenda
MA BBO No. 550587
Andrew Loewenstein
MA BBO No. 648074
155 Seaport Boulevard
Boston, MA 02210
(617) 832-1000
chart@foleyhoag.com
adm@foleyhoag.com
aloewenstein@foleyhoag.com

ELECTRONIC FRONTIER FOUNDATION
David Greene
CA Bar No. 160107
Sophia Cope
CA Bar No. 233428
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
davidg@eff.org

CENTER FOR JUSTICE AND ACCOUNTABILITY
Daniel McLaughlin (*pro hac vice pending)*
CA Bar No. 315326
Claret Vargas *(pro hac vice pending)*
MA BBO No. 679565
Carmen Cheung Ka Man *(pro hac vice pending)*
NY Bar No. 4132882
268 Bush St. #3432
San Francisco, CA 94104
(415) 544-0444
dmclaughlin@cja.org
cvargas@cja.org
ccheung@cja.org

Attorneys for Plaintiff Loujain Hathloul Alhathloul